UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/718,734	11/22/2000	George M. Brookner	770P009595-US(PAR)	2840

2512	7590	07/12/2004

PERMAN & GREEN
425 POST ROAD
FAIRFIELD, CT 06824

EXAMINER
LEMMA, SAMSON B

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 07/12/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
Office Action Summary	09/718,734	BROOKNER ET AL.
	Examiner	Art Unit
	Samson B Lemma	2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _22 November 2000_.
2a)☐ This action is **FINAL.**   2b)☒ This action is non-final.
3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-30_ is/are pending in the application.
    4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5)☐ Claim(s) _____ is/are allowed.
6)☒ Claim(s) _1-30_ is/are rejected.
7)☐ Claim(s) _____ is/are objected to.
8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.
10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.
    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
    a)☐ All b)☐ Some * c)☐ None of:
      1.☐ Certified copies of the priority documents have been received.
      2.☐ Certified copies of the priority documents have been received in Application No. _____.
      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
        application from the International Bureau (PCT Rule 17.2(a)).
    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3)☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _5 & 6_.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .
5)☐ Notice of Informal Patent Application (PTO-152)
6)☐ Other: _____.

DETAILED ACTION

1.   Claims 1-30 have been examined.

Claim Rejections - 35 USC § 112

2.   The following is a quotation of the second paragraph of 35
U.S.C. 112:

> The specification shall conclude with one or more claims
> particularly pointing out and distinctly claiming the subject
> matter which the applicant regards as his invention.

3.   Claim 1 and 21 are rejected under 35 U.S.C. 112, second
paragraph, as being indefinite for failing to particularly point
out and distinctly claim the subject matter which applicant
regards as the invention. Claim 1 and 21 recite the limitation
"standard". Applicant did not define the term "standard"
distinctly in the claim. The term "standard" has to explicitly be
defined in both claims 1 and 21 so that there would not be any
ambiguity.

4.   Claims 3-12 depend from rejected claim 1, and include all
the limitations of the respective claim, thereby rendering those
dependent claims indefinite.

5.   Claims 22-24 depend from rejected claim 21, and include all
the limitations of the respective claim, thereby rendering those
dependent claims indefinite

6.   Claim 14 is rejected under 35 U.S.C. 112, second paragraph,
as being indefinite for failing to particularly point out and
distinctly claim the subject matter which applicant regards as
the invention. Claim 14 recites the limitation said
"communication channel". There is ambiguity since it does not
explain which communication channel it is. The "communication
channel" could be the one that is used to provide the device to
the user or the other one that is used to communicate the PIN to
the user of the device. The communication channel has to be
clearly one or the other.

7.   Claims 15 depend from rejected claim 14, and include all
the limitations of the respective claim, thereby rendering those
dependent claims indefinite.

8.   Claim 22 recites the limitation said encrypted version of
said PIN. There is insufficient antecedent basis for this
limitation in the claim.

9.   Claims 23-24 depend from rejected claim 22, and include all

the limitations of the respective claim, thereby rendering those

dependent claims indefinite

Claim Rejections - 35 USC § 102

10.   The following is a quotation of the appropriate paragraphs

of 35 U.S.C. 102 that form the basis for the rejections under

this section made in this Office action:

A person shall be entitled to a patent unless -

(e) the invention was described in (1) an application for patent,
published under section 122(b), by another filed in the United States
before the invention by the applicant for patent or (2) a patent granted
on an application for patent by another filed in the United States before
the invention by the applicant for patent, except that an international
application filed under the treaty defined in section 351(a) shall have
the effects for purposes of this subsection of an application filed in
the United States only if the international application designated the
United States and was published under Article 21(2) of such treaty in the
English language.

11.   Claims 27-30 are rejected under 35 U.S.C. 102(e) as

being unpatentable over Challender et al.(hereinafter refereed to

as Challender) (U.S. Patent No.6,668,323).

12.   As per claim 27, Challender discloses a method for

resetting a pin in a secure device comprising:

(a) sending a request message to a data center having an

original pin (understood by the examiner as power on

password POP) for said device(said device understood by the

examiner to be a computer system) said request message

including authorization data indicative of at least one of

the device and an authorized user of said device, (column

5, 23-44) (serial number meets the recitation of the data

indicative of the device)

and

(b) Securely communicating the original PIN to the

location of the device (column 5, lines 39-44)(the computer

system understood be the said device by the examiner)

13.   As per claim 28, Challender discloses the method as applied

to claim 27 above. Furthermore, Challender discloses the method

wherein the device has the current PIN, further comprising

replacing the current PIN with the Original PIN.(column 5, lines

29-51; figure 4; column 4, lines 21-22; column 4, lines 54-58).

14.   As per claim 29, Challender discloses the method as applied

to claim 27 above. Furthermore Challender discloses the method

wherein the communicating of the original PIN comprises:

> sending the Original PIN to the user of the
>
> device;(column 5, 39-40) and

> the user of the device entering the Origional PIN into
>
> the device.(column 5, line, lines 50-51 and figure 4).

15.   As per claim 30, Challender discloses the method as applied

to claim 27 above. Furthermore, Challender teaches the method

wherein at least one of (a) and (b) are performed using at least

one of a secure communication channel and secure communication

techniques.(column 5, lines 23-24; column 5, lines 39-44).

Claim Rejections - 35 USC § 103

16.   The following is a quotation of 35 U.S.C. 103(a) which

forms the basis for all obviousness rejections set forth in this

Office action:

> (a) A patent may not be obtained though the invention is not identically
> disclosed or described as set forth in section 102 of this title, if the
> differences between the subject matter sought to be patented and the
> prior art are such that the subject matter as a whole would have been
> obvious at the time the invention was made to a person having ordinary
> skill in the art to which said subject matter pertains. Patentability
> shall not be negatived by the manner in which the invention was made.

17.   Claims 1-12 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Markus G. Kuhn (hereinafter refereed to as

Kuhn) (reference U)(07/30/1997) in view of Matyas et al

(hereinafter refereed to as Matyas)(U.S. Patent No. 4,924,514).

18.   As per claim 1, Khun teaches a method for generating PIN

comprising:

   Generating a number of random binary bits (this number is

   transferred in to a 64-bit pattern and meets the limitation

   of random bits);(Page 1, lines 12-17; figure on the last

   page)

   Determining any arbitrary digits out of the 16 hexadecimal

   digit (take 3-6 hexadecimal digits), (meets the limitation

   of determining the least significant bits).(page 1, lines

   17, page 4; figure on the last page)

   Converting the hexadecimal digit (3-6) in to a decimal

   integer using a decimalization mapping (Figure on the last

   page)(this meets the limitation of converting the least

   significant bits to a decimal integer).

Furthermore Kuhn teaches shifting the values of the integer

by a predetermined (selected) constant to produce a shifted

integer (constant is an offset in the reference) (figure on

the last page).Kuhn does not explicitly teaches encoding

the shifted integer as bits in a PIN block in accordance

with a standard. ("standard" is understood by the examiner

to be "ISO 9564-1"). However Matyas teaches encoding the

pin in a pin block in accordance with one of the several

industry-accepted de facto standard.(standard could be ISO

9564-1)(column 7,lines 52; column 5, lines 53-55 and column

5, line 63-67).

Therefore it would have been obvious to one having ordinary

skill in the art at the time of the invention was made to

encode kuhn's shifted integer as per teaching of Matya's,

in order to produce the encoding PIN block in accordance to

the industry accepted de facto standard (standard could be

ISO 9564-1)

19.   As per claim 2, the combination of khun and Matyas teach

the method as applied to claim 1 above. Furthermore, Matyas

teaches the method wherein the standard is one of industry

accepted de facto standards.(standard could be ISO 9564-1)

(column 5,line 65-68 and column 6, line 1).

20. As per claim 3, the combination of Kuhn and Matyas teach the method as applied to claim 1 above. Furthermore, Kuhn teaches the method wherein the number of bits is sixty-four (64-bit pattern) or which is equivalent to the 16-digit decimal number.(page 1,lines 12-15; figure on the last page).Kuhn discloses that the 64 bits pattern or its equivalent 16-digit decimal number is formed by concatenating five digits of the bank routing number, ten digit account number, and a single digit card sequence number and after that the result was encoded (encrypted) using the DES algorithm with the secret 56-bit institute key k1.(page1, lines 12-17; figure on the last page).(this will make each successive digit or bits to be equally likely and unpredictable to meet the recitation of Random.)

21. As per claim 4, the combination of Kuhn and Matyas teach the method as applied to claim 1 above. Furthermore, Kuhn teaches the method wherein the number of bits are sixteen or (4 decimal integer).(taking 3-6 digits or its equivalent 4 decimal integer).(page 1, lines 17). selecting any sixteen bits out of the 64 bits or any 4 hexadecimal digit out of the 16 hexadecimal digit is arbitrary. Selection the right most, or the middle or the left most bits is arbitrary. (Khun disclosure meet the recitation of sixteen least significant bits

22. As per claim 5, the combination of Kuhn and Matyas teach the method as applied to claim 1 above. Furthermore Kuhn teaches the method wherein the constant is the offset 1707). (figure on the last page). Kuhn also discloses replacing the 1st digit by 1, if the first of those digits is a 0, to make sure that the leading digit is not equal to 0.(page 1, line 18; figure on the last page)(This meets the recitation for the constant.

23. As per claim 6-11 the combination of kuhn and Matyas teach the method as applied to claim 1 above. Furthermore Matyas teaches the method wherein the PIN block includes the PIN block formats which have been standardized or have become industry-accepted de facto standards.(standard could be ISO 9564-1)(column 5,lines 63-68; column 6,lines 1-19 and column 7,line 53).

24. As per claim 12, the combination of kuhn and Matyas teach the method as applied to claim 1 above. Furthermore Kuhn teaches the method wherein the number of bits is sixty-four (64-bit pattern) or which is equivalent to the 16-digit decimal number.(page 1,lines 12-15; page4(last page)).Kuhn also teaches that bits or its equivalent 16-digit decimal number is formed by concatenating five digits of the bank routing number, ten digit account number, and a single digit card sequence number and finally the result was encoded (encrypted) using the DES algorithm with the secret 56-bit institute key.(page1, lines 12-

17; page 4).(This will meet the recitation of pseudorandom
generation).

25.   Claims 13-19, 25-26 are rejected under 35 U.S.103(a) as
being unpatentable over Holch et al. (hereinafter refereed to as
Holch) (U.S. Patent No. 6,280,328) in view of Matyas et al
(hereinafter refereed to as Matyas)(U.S. Patent No. 4,924,514).

26.   As per claim 13, Holch discloses a method for managing
security of a PIN used to provide access to a secure device,
comprising:

> choosing the PIN;(column 6, 20-21)
>
> storing an encrypted version of the PIN in the
> device;(column 6,21-24) and
>
> Furthermore Holch teaches communicating PIN to the
> account server after encrypting the PIN (column
> 7,lines 16-19). Holch does not explicitly teach
> communicating the PIN to a user of the device via a
> communication channel separate and apart from a
> channel used to provide the device to the user.
> However Matyas discloses communicating the PIN to a
> user of the cardholder via a communication channel
> (mail) separate and apart from a channel used to
> provide the card (device) to the user.(figure 5,
> column 4, lines 57-62).Therefore it would have been

obvious to one having ordinary skill in the art at the

time of the invention was made to communicate the

Holch's PIN as per teachings of Matyas to communicate

the PIN to a user of the device via a communication

channel separate and apart from a channel used to

provide the card (device) to the user, in order to

ensure that the PIN is delivered to the actual user

safely and securely.

27.   As per claim 14, the combination of Holch and Matyas teach

the method as applied to claim 13 above. Furthermore Matyas

teaches the method wherein the standard said communication

channel is a secure channel.(figure 5, column 4, lines 57-62)

28.   As per claim 15, the combination of Holch and Matyas teach

the method as applied to claim 14 above. Furthermore Matyas

teaches the method comprising using encryption to render said

communication channel secure.(figure 5; column 4, lines 57-62).

29.   As per claim 16, the combination of Holch and Matyas teach

the method as applied to claim 13 above. Furthermore Matyas

teaches the method wherein the user of said device chooses said

PIN.(column 6, line 20-21).

30.   As per claim 17, the combination of Holch and Matyas teach the method as applied to claim 16 above. Furthermore Holch teaches a method wherein a manufacturer of said device causes said encrypted version of said PIN to be stored in said device.(column 6,21-24).

31.   As per claim 18 and 19 the combination of Holch and Matyas teach the method as applied to claim 17 above. Furthermore Holch teaches the method further comprising the manufacturer or the card (device) issuer storing a record of said PIN in the Account server(column 6, lines 29-31). Therefore It is also obvious for one having ordinary skill in the art at time of the invention to consider that the card (device) issuer has a capability of discarding all the records of said PIN if it has the capacity of storing a record of PIN.

32.   As per claim 25 and 26 the combination of Holch and Matyas teach the method as applied to claim 13 above. Furthermore Holch teaches the method wherein the said device (magnetic card) stores the value of funds.(colum 6, 37-44).

33.   Claims 20-24 are rejected under 35 U.S.103(a) as being unpatentable over Holch et al. (hereinafter refereed to as Holch) (U.S. Patent No. 6,280,328) in view of Matyas et al (hereinafter refereed to as Matyas)(U.S. Patent No. 4,924,514) as applied to

claim 13 above and further in view of Markus G. Kuhn (hereinafter

refereed to as Kuhn) (reference U) (07/30/1997)

34.   As per 20, the combination of Holch and Matyas teach a

method wherein said PIN is chosen either by the user of the

device or the PIN is generated and communicated to the user of

the device. The combination of Holch and Matyas does not

explicitly teach that the PIN is chosen using a random process.

However, Kuhn teaches that bits or its equivalent 16-digit

decimal number is formed by concatenating five digits of the bank

routing number, ten digit account number, and a single digit card

sequence number and finally the result was encoded (encrypted)

using the DES algorithm with the secret 56-bit institute key.

(page1, lines 12-17; page 4).Therefore it would have been obvious

to one having ordinary skill in the art at the time the invention

was made to combine the teachings of Holch and Matyas related to

choosing a PIN so as to include the initiation to choose the PIN

in random process as per teachings of Khun, because such

modification will make the PIN to be chosen by a random process.

Therefore It would have been obvious to employ the teachings of

Khun within the combination of Holch and Matyas to obtain the

claimed invention.

35.   As per claim 21 the combination of Holch, Matyas and Khun

teaches the method as applied to claim 20 above. Furthermore

Khun teaches method wherein said PIN is choosen by:

Generating a number of random binary bits (this number is

transferred in to a 64-bit pattern and meets the limitation

of random bits);(Page 1, lines 12-17; figure on the last

page)

Determining any arbitrary digits out of the 16 hexadecimal

digit (take 3-6 hexadecimal digits), this meets the

limitation of determining the least significant bits).(page

1, lines 17, page 4; figure on the last page)

Converting the hexadecimal digit (3-6) in to a decimal

integer using a decimalization mapping (Figure on the last

page)(this meets the limitation of converting the least

significant bits to a decimal integer).

Furthermore Kuhn teaches shifting the values of the integer

by a predetermined (selected) constant to produce a shifted

integer (constant is an offset in the reference) (figure on

the last page).Kuhn does not explicitly teaches encoding

the shifted integer as bits in a PIN block in accordance

with a standard. ("standard" is understood by the examiner

to be "ISO 9564-1"). However Matyas teaches encoding the

pin in a pin block in accordance with one of the several

industry-accepted de facto standard.(standard could be ISO

9564-1)(column 7,lines 52; column 5, lines 53-55 and column

5, line 63-67).

Therefore it would have been obvious to one having ordinary

skill in the art at the time of the invention was made to

encode kuhn's shifted integer as per teaching of Matya's,

in order to produce the encoding PIN block in accordance to

the industry accepted de facto standard (standard could be

ISO 9564-1)

36.   As per claim 22, the combination of Holch, Matyas and

Khun teaches the method as applied to claim 21 above.

Furthermore Holch teaches a method wherein a manufacturer

of said device causes said encrypted version of said PIN to

be stored in said device.(column 6,21-24).

37.   As per claim 23 and 24 the combination of Holch,

Matyas and Khun teaches the method as applied to claim 21

above. Furthermore Holch teaches the method further

comprising the manufacturer or the card (device) issuer

storing a record of said PIN in the Account server(column

6, lines 29-31). Therefore It would have been obvious for

one having ordinary skill in the art at time of the invention was made to consider that the card (device) issuer has a capability of discarding all the records of said PIN if it has the capacity of storing a record of PIN.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 703-305-8745. The examiner can normally be reached on Monday-Friday (8:00 am---4:30 pm).
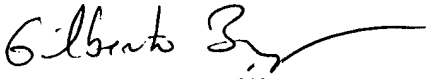
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 703-305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be
obtained from the Patent Application Information Retrieval (PAIR)
system. Status information for published applications may be
obtained from either Private PAIR or Public PAIR. Status
information for unpublished applications is available through
Private PAIR only. For more information about the PAIR system,
see http://pair-direct.uspto.gov. Should you have questions on
access to the Private PAIR system, contact the Electronic
Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA

June 28, 2004

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100